УДК 004.056(574)

А. Н. Камбаров, Н. А. Тулаганов

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

В данной работе представлены проблемы обеспечения информационной безопасности Казахстана. Рассмотрены современные аспекты обеспечения информационной безопасности Республики Казахстан. Развитие государства и общества как политико-правовых явлений осуществляется всегда в четко определенных исторических и территориальных факторах, которые обусловливают это развитие. При этом угрозы для государства, общества и человека также находятся в постоянном изменении, адекватном развитию общества и государства. Современные мировые тенденции сегодня сигнализируют о возникновении новых форматов угроз для национальной безопасности Казахстана в XXI в.

Ключевые слова: *информация, информационные технологии, информационная безопасность.*

This paper presents the problem of information security Kazakhstan. The modern aspects of information security of the Republic of Kazakhstan.Development of the state and society as a political and legal phenomena is always carried out in well-defined historical and regional factors that cause this development. At the same time a threat to the state, society and man are also in constant change, adequate development of the society and the state. Modern global trends today signaled the emergence of new formats threats to the national security of Kazakhstan in the XXI century.

Keywords: *information, information technologies, information security.*

Проблема информационной безопасности публики на сегодняшний день стала стратегической проблемой, которая включает в себя комплексные понятия — «международная безопасность» и «национальная безопасность». Информационная безопасность включает в себя три составляющие: требования, политику и механизмы. Требования характеризуют цели защиты. Они могут отвечать на такой вопрос как: «Что вы хотите от вашей безопасности?». Политика характеризует значение защиты. Это значение должно отвечать на вопрос: «Какие мероприятия должны быть осуществлены в достижении поставленных целей?». Механизмы безопасности должны предопределять ее политику [2].

Национальная безопасность рассматривается в нюансе общественно-финансового развития страны как стратегия государственная, производимая для сохранения и защиты технических и языковых данных, предотвращения информационных войн [3]. Представление и изучение данных явлений, формирование граней противодействия — главные проблемы, решение которых обусловлено направлением всей системы национальной безопасности.

Актуальность проблемы обеспечения информационной защиты информации обусловлена в первую очередь, тем, что в современном обществе данные стали стратегическими национальными ресурсами. За минувшие годы в Республике Казахстан выполнен ряд мер по совершенствованию концепции обеспечения информационной защищенности страны. В соответствии со Стратегией национальной безопасности Республики Казахстан была разработана и утверждена Концепция информационной безопасности [4], которая предусматривает реализацию комплекса законных, организационных и научно-промышленных мероприятий, направленных на мониторинг, выявление, предупреждение и предотвращение угроз в области информационной безопасности. Технический прогресс в областях микроэлектроники, аппаратных и программных средств, а также вычислительной техники делает процесс развития информационных технологий быстрым и оказывает большое влияние на их совершенствование.

Развитие, связанное с информатизацией всех аспектов государственной и социальной жизни, объективно говорит о том, что существование современного независимого государства неразрывно связано с обеспечением информационной безопасности всех звеньев его муниципальных структур. Анализ и исследование мирового опыта показывает, что непосредственно в последние несколько лет случилось качественное изменение в процессе управления всеми уровнями: от межгосударственных образований до личных фирм и банков. В это же время одновременно развивалась и усиливалась опасность несанкционированного доступа к информации с целью получения данных и нарушения их функционирования. Подобная угроза совершенно неоспорима, потому как разрушение и расстройство информационной инфраструктуры страны соизмеримы по силе воздействия с результатами реальных военных операций. Соответствующими должны быть и мероприятия по предупреждению таких последствий. Эффективно противодействовать информационным угрозам в современных условиях способна лишь хорошо организованная государственная система обеспечения информационной безопасности, осуществляемая при абсолютном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан.

К внутренним атакам информационной защиты относятся:

– направленное изменение данных, целью которого является отрицательное общественное мнение и побуждение принятия необдуманного политического решения;

– невысокая техническая укомплектованность линий связи и их охрана;

– неудовлетворительная степень качества информационных, телекоммуникационных ресурсов, снижение значимости и ненадлежащее обеспечение всех прав негосударственных печатных, теле- и радиокомпаний на приобретение и распространение данных;

– компьютерные правонарушения.

Для надлежащего решения задачи обеспечению информационной безопасности в Казахстане, на наш взгляд, необходимо наличие единой политики взаимодействия государственных органов с индивидуальным сектором и средствами массовой информации.

Используя правила, можно добиться высокого результата в области защиты информационной безопасности.

В некоторых случаях можно использовать и традиционные средства защиты или компенсировать отсутствие специализированных решений дополнительными техническими и организационными мерами, которые могут повлечь за собой дополнительные риски, связанные с человеческим фактором, необходимостью увеличения количества требуемых ресурсов и проблемами совместимости.

Например, для защиты виртуальных машин могут применяться антивирусные средства, которые уже используются в компании. В этом случае необходимо более тщательно подойти к составлению расписания, по которому будут проверяться виртуальные машины. Таким образом можно избежать критической загрузки виртуальных серверов.

Еще один момент, на который стоит обратить внимание, — применение средств контроля несанкционированного доступа. Практически все проблемы в этой области возникают из-за невыполнения рекомендаций производителей платформ виртуализации. Документы, в которых четко описаны действия администратора по безопасности, имеются для множества платформ виртуализации. Часть из них выпущена самими производителями, часть — экспертными сообществами. Например, подобные руководства предостерегают от использования встроенных «по умолчанию» в платформу ролей. Перед началом работы необходимо составить матрицу доступа и уже по ней сформировать требуемые для работы с виртуализированной инфраструктурой роли.

Особую роль при построении системы обеспечения безопасности виртуализированных и гибридных инфраструктур (имеющих в своем составе как виртуализированные, так и физические сегменты инфраструктуры) играют сетевые средства защиты. Одним из объектов воздействия на виртуализированную инфраструктуру могут служить сетевые каналы взаимодействия виртуальных машин и внешние сетевые каналы управления виртуализированной инфраструктуры [6]. При этом важно понимать, что такие средства защиты широко представлены на рынке, но мы рассматриваем только те средства защиты сети, которые специально предназначены для виртуализированных инфраструктур и заявлены самим разработчиком.

Очень важно рассмотреть общие защиты виртуализации, какими принципами руководствоваться при выборе специализированных средств защиты? Правила помогут осуществить цель. Существует несколько основных правил:

1. Необходимо помнить, что большая часть из этих средств защиты не является специализированными средствами для виртуализированной инфраструктуры, а представляет собой лишь адаптированные средства защиты для работы

в виртуальной среде. Такие решения работают внутри виртуальной машины, так же как и на физическом сервере, не зная о своем виртуальном окружении и не позволяя бороться со специфическими угрозами и уязвимостями виртуальной инфраструктуры. Сложность возникает в том, чтобы отличить одно решение от другого.

2. Необходимо рассматривать функционал продукта и проверять, как он реализуется на практике. Рекомендуется посетить специализированные интернет-ресурсы, где специалисты обмениваются опытом и обсуждают сильные и слабые стороны конкретного продукта.

3. Необходимо учитывать, для каких конкретно платформ виртуализации (и их версий) предназначено средство защиты.

4. При выборе сертифицированных продуктов необходимо обращать внимание на технические условия, по которым этот продукт прошел сертификацию. В них должны быть прописаны: среда тестирования, ограничения по эксплуатации и функционал, на который выдан сертификат.

Используя правила, можно добиться высокого результата в области защиты информации. Другой вариант использования виртуализации рабочего места — это усиление контроля организации за пользовательской средой [7]. Организация хранит хорошо известный образ, который содержит операционная система (ОС) и все приложения, необходимые пользователю. Пользователь загружает образ и выполняет все работы внутри этого образа, не на хостовой ОС, и затем покидает гостевую ОС. Позже, пользователь перезагружает гостевую ОС, чтобы сбросить все предыдущие изменения. Преимущества такой стратегии в том, что вредоносные изменения, которые были допущены в работе, или установленное вредоносное ПО будут стерты при выходе.

При виртуализации рабочего места, пользовательские данные в нормальном режиме хранятся на хосте или в сети, иначе бы они просто терялись при каждом выходе пользователя из системы. Этот пункт может стать наиболее сложным и отталкивающим пользователей: очень легко сохранить новый документ в том месте, где он был создан, и только позже обнаружить, что документ потерян из-за того, что был сохранен не в той директории [8]. Некоторые системы виртуализации рабочего места имеют методы, удостоверяющие, что пользовательские данные корректно сохранены перед выходом, но подобные методы не являются надежными.

Среда виртуализации — это особый программно-аппаратный слой в инфраструктуре компании, который отличается от традиционной физической архитектуры наличием абсолютно новых составляющих: гипервизора, средств управления и обслуживания виртуализированной инфраструктуры. Ключевым элементом архитектуры среды виртуализации является гипервизор.

Он обеспечивает осуществление нескольких операционных систем, их изоляцию друг от друга и разделение ресурсов между ними. Получив контроль над гипервизором, злоумышленник приобретает практически неограниченные возможности: он незаметно для средств защиты, установленных в виртуальных машинах,

может перехватывать данные. Фактически именно эти составляющие становятся основными объектами атак виртуализированной инфраструктуры, т. к. компрометация гипервизора может привести к компрометации всех виртуализированных серверов и рабочих станций, а захват средств управления виртуализированной инфраструктуры поставит под угрозу всю инфраструктуру компании. Следовательно, вместе с плотностью размещения виртуальных машин растут и риски. В связи с этим защита составляющих виртуализации является ключевой задачей в общей стратегии защиты информации в виртуализированной инфраструктуре.

Классический пример определяет возможности для эффективного понимания процесса. Предположим, что одна служба содержит критичную информацию и защищается очень хорошо, тогда другая служба на том же хостинге содержит маловажную информацию и защищается соответственно слабее. Атакующий, который хочет завладеть критичной информацией, может сначала успешно проатаковать слабо защищенную службу и затем, используя уже тот факт, что он внутри виртуальной сети, попытаться получить доступ к критичной службе или провести атаку на гипервизор, что также предоставит возможность доступа к этой службе.

Организации, которые имеют политики, относящиеся к распределению вычислительных ресурсов, должны учитывать виртуализацию в таких политиках.

Виртуализация используется для запуска серверов на множестве хостов и для миграции серверов от хоста к хосту, основанной на изменяющихся потребностях в ресурсах, это называется облачными вычислениями. Облачные вычисления — это «модель удобного подключения по требованию сетевого доступа к общему набору настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ, приложений и услуг), которые могут быть быстро предоставлены с минимальными управляющими усилиями со стороны поставщика услуг».

Одна из наиболее общих причин использования виртуализации рабочего места — это возможность пользователя запускать приложения для разных ОС на одном хосте. Без виртуализации это можно было бы реализовать использованием множества устройств, отдельного для каждой ОС, или настройкой одного устройства загружаться с разных ОС и использовать только одну ОС одновременно. Виртуализация позволяет пользователю иметь доступ к нескольким ОС одновременно на одном компьютере. Гипервизор полной виртуализации инкапсулирует все компоненты гостевой ОС, включая ее приложения и виртуальные ресурсы, в одну логическую сущность. Образ — это файл или директория, которая содержит, как минимум, эту инкапсулированную информацию. Образы хранятся на жестких дисках и могут быть перенесены на другую систему так же как и любой файл. Некоторые системы виртуализации используют для образов стандарт, называемый Open Virtualization Format (OVF), который обеспечивает независимость образа от платформы виртуализации [9].

Снимок (snapshot) — это запись состояния запущенного образа, обычно в виде отличий между образом и текущим состоянием. Например, снимок будет

записывать изменения в виртуальном хранилище, виртуальной памяти, сетевых подключенях и т. п. Снимки позволяют гостевым ОС быть остановленными, а затем возобновленными без выключения или перезагрузки. Многие, но не все системы виртуализации могут делать снимки.

На некоторых гипервизорах снимки гостевых ОС могут быть возобновлены (запущены) на разных хостах. Правда, здесь может возникнуть ряд проблем при обработке живой миграции (live migration/real-time migration), включая задержку передачи и любые различия между двумя физическими серверами (например, IP-адрес, число процессоров или количество дискового пространства), но большинство решений имеют механизмы решения этих проблем. Если на целевой системе развернуто то же средство виртуализации, многие из этих проблем не возникнут. Тем не менее, живая миграция даже в однородной среде — это потенциальные конфигурационные ошибки, которые могут повлиять на безопасность гостевых ОС.

Литература

1. *Geer D., Hoo K., Jaquith A.* Information Security: Why the Future Belongs to the Quants // IEEE Security & Privacy. Vol. 1. No. 4. July/August 2003. P. 24–32.
2. *Bishop M.* What Is Computer Security? // IEEE Security & Privacy. Vol. 1. No. 1. January/February 2013. P. 67–69.
3. *Gliedman C.* Managing IT Risk with Portfolio Management Thinking // CIO (Analyst Corner). URL: www.cio.com/analyst/012502_giga.html.
4. *Махмутов А.* Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешнеполитические перспективы и новые концепты международной стратегии Казахстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан — Лидера Нации. 2012. 12 марта. URL: iwep.kz/index.
5. *Дмитриенко Т. А.* Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // ANALYTIC: информационно-аналитический журнал. 2013. № 5. С. 12–14.
6. *Стрельцов А. А.* Актуальные проблемы обеспечения информационной безопасности // Технологии безопасности. № 11. С. 54.
7. Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан „О Концепции информационной безопасности Республики Казахстан до 2016 года“» (утвержден) // Электронная база нормативно-правовых актов «Параграф». URL: online.zakon.kz.
8. Информационная безопасность. Комитет национальной безопасности Республики Казахстан [Электронный ресурс]. URL: http://www.knb.kz/
9. *Колоскова Г.* Модели и алгоритмы реконфигурации многопроцессорных систем. Курск: Курский гос. техн. ун-т, 2004. 257 с.
10. *Takanami I.* Built-in Self-Reconfiguring Systems for Fault Tolerant Mesh-Connected Processor Arrays by Direct Spare Replacement // Proc. IEEE Intern. Symp. Defect and Fault Tolerance in VLSI Systems. 2001. P. 134–142.